UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/697,421	08/23/96	MOVALLI M	06555.0001-0

MM32/0719

FINNEGAN HENDERSON FARABOW GARRETTAND
DUNNER LLP
1300 I STREET NW
WASHINGTON DC 20005

EXAMINER	
TREMBLAY,M	
ART UNIT	**PAPER NUMBER**
2876	

DATE MAILED: 07/19/99

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	Application No. 08/697,421	Applicant(s) Moralli et al.
	Examiner Mark Trembley	Group Art Unit 2876

—The MAILING DATE of this communication appears on the cover sheet beneath the correspondence address—

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, such period shall, by default, expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Status

☐ Responsive to communication(s) filed on _____.

☒ This action is **FINAL.**

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle,* 1935 C.D. 1 1; 453 O.G. 213.

Disposition of Claims

☒ Claim(s) 1-27 and 29-31 is/are pending in the application.

Of the above claim(s) _____ is/are withdrawn from consideration.

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) 1-27 and 29-31 is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claim(s) _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The proposed drawing correction, filed on _____ is ☐ approved ☐ disapproved.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119 (a)-(d)

☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 11 9(a)-(d).

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) _____.

☐ received in this national stage application from the International Bureau (PCT Rule 1 7.2(a)).

*Certified copies not received: _____.

Attachment(s)

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

☐ Interview Summary, PTO-413

☐ Notice of Reference(s) Cited, PTO-892

☐ Notice of Informal Patent Application, PTO-152

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Other _____

Office Action Summary

Part III Action on the Merits

Response to Amendment

Applicants amendment dated 3/29/99 has been entered as paper number 11 and has been duly considered.

Claim Objections

Claims 3, 4, and 14 are objected to because of the following informalities: while the claims recite a "storage means" which is the essentially the same statement as a "memory means" in this context, "the memory means" should be changed to "the storage means" for positive agreement with the antecedent term. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.
>
> This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1-4, drawn to methods for generating transactions, and claims 24-27, drawn to a system for generating secure endorsed transactions, are rejected under 35 U.S.C. § 103 as being unpatentable over Donald W. Davies "Use of the 'Signature Token' to Create a Negotiable Document ("Davies" hereinafter) in view of "in view of U.S. Patent #4,825,050 to Griffith et al. ("Griffith" hereinafter) . Davies discloses a computer implemented (page 378, under the heading "The Signature Token", e.g. the description of a smart card which has a "microprocessor")

method of generating secure endorsed transactions (see description on page 378 under the heading "The Signature Token", e.g. the description of debit cards, credit transactions, etc.), the method comprising:

receiving transaction data (9, 10, 11, 12, 14, and 15) corresponding to a transaction and at least one unique identifier of a customer (typically a human) (5); and

generating a unique code 16 from the transaction data and the unique identifier of a customer, wherein the unique code constitutes a secure endorsement of the transaction by the party corresponding to the unique identifier (5).

Davies discloses the features of the invention as described above, but does not teach that a "human" identifier, e.g. a biometric, can be used with such an encryption scheme to further enhance security. Griffith teaches that " Multiple inputs are accepted in the following manner: The individual information record 101 which is the data to be 'locked'; the individual identifier 100 which may be some characteristic of the individual e.g. finger, voice, or retinal pattern, signature, or chemical structure or some information known only to the individual, e.g. a combination, pass word or phrase; a private key 110 which is known only to the issuing entity and which is generated by any method 109 meeting the criteria for public key crypto systems outlined by W. Diffie and M.E. Hellman in their article cited above such as the system publicly disclosed by Rivest, Shamir, and Adleman ob cit; and optionally other data 113 which is necessary or convenient to include regarding the application made of the present method." Thus, Griffith teaches that the public/private key method can be used with a "human identifier" to thwart fraud. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to include a "human identifier" as taught by Griffith in the system taught by Davies because this would make it more difficult for a thief to use a stolen smart card, as taught by Griffith to create the negotiable documents taught by Davies.

Re claim 25, Official Notice is taken that a card insertion sensor is notoriously old and well known in the art. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to use a card insertion sensor in a smart card system according to Davies and Even so that when a card is inserted into the device, the transaction can begin automatically, making the user's task easier, and speeding the transaction.

Claims 5-23 and 29-31 are rejected under 35 U.S.C. § 103 as being unpatentable over Davies in view of U.S. Patent #4,825,050 to Griffith et al. ("Griffith" hereinafter) and further in view of U.S. Patent #5,689,565 to Spies ("Spies" hereinafter). Davies and Griffith do not explicitly teach a network implementation or a need for a receipt, as mentioned above. A network implementation for a system like this is common. Spies provides an example of a networked system used for an application similar to the combined teachings of Davies and Griffith. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to use a method according to the combined teachings of Davies and Griffith in a networked environment taught by Spies, because networked environments allow for the greater flexibility in performing transactions, as was commonly and well understood in the art.

Response to Arguments

Applicant asserts at page 4 of the amendment that "there is no teaching or suggestion by Davies that the identity of either the customer or beneficiary of the check are unique." Examiner respectfully disagrees. Uniqueness is inherent to identity in this context. If the identitity of the customer or beneficiary is not unique, then the customer is not actually identified by the customer identity. If the clearing house cannot determine a unique beneficiary for each check, then it would not be able to perform any valid accounting. The Applicant appears to believe that "customer identity" might mean the same thing as "customer's given name", such as "John Smith". A fair reading of Davies would not allow this interpretation. Instead, customer identity must be interpreted as a unique number which reliably and uniquely identifies a single customer. If the customer identity is not unique, the incorrect assignment of funds is inevitable.

Applicant makes a similar argument at pages 4-5 with respect to the uniqueness of the digital signature and digital signal of Davies. Examiner respectfully disagrees, for similar reasons. Moreover, the Applicant's claimed invention is substantially the same as Davies. The customer identity is unique, as stated above. The customer's public key is unique, for the same reasons that the customer's identity is unique. The transaction data, by virtue of containing a number unique to the customer, a number unique to the beneficiary, and a number unique to the transaction for the given customer (the check sequence number), a date and a time, is itself a unique number. For

example, "customer 4165423123459876 writing debit check number 4876 to beneficiary 9876475873648746 for $142.05 US dollars on 04/11/1999 at 04:13 am for 'insomnia medication'". Thus, the transaction data, numbers 9-15, unquestionably form a unique number (a digital number which represents the above string in a binary code such as ascii). The appended signature on the check is the unique number formed by items 9-15 encrypted using the unique (see page 380, second line of the 4th paragraph of Davies) customer secret key (which must be a very long number itself, in order to satisfy public key security needs). Most importantly, the number generated in this process, 16, is a **digital signature**. It definitely constitutes a secure endorsement of the transaction by the party corresponding to the human identifier.

Should the Applicant argue that there is a finite chance that the number generated in the signature process is the same as another number generated as a signature in another transaction, Examiner would point out that there is likewise a finite chance of such an occurance with Applicant's preferred embodiment of the invention. The finite chance is both negligible, because of the size of the numbers involved (think of the state lotteries, which is at best merely a tiny 12 digit number-- the solar system may collapse before such a match occurs by chance in a reasonably robust implementation of Davies), and effectively irrelevant when it is considered as an appendage to the transaction. The transaction is always a unique number, so that the digital signature appended to the transaction data is inherently a unique number.

Applicant asserts that Even does not correct the alleged deficiencies of Davies. The point is essentially moot, but Even uses unique numbers for the same reasons as outlined above.

Applicant also argues against the applicability of the teachings of Griffith because the method used by Griffith is used to "lock" data. Applicant states:

"The closest allegory to the concept of "locking" information using a identifier in Davies relates to the use of a PIN number to access information stored within the 'smart card', which cannot be accessed without the PIN number (first paragraph of page 379)." Examiner disagrees with these statements, and the line of reasoning which ensues from them. Griffith states in column 2, lines 28-29, "The term 'lock' and encrypt are interchangeable. The term 'unlock' and decrypt are interchangeable." There is no equivocation here, nor any reference to the use of a PIN number. The Applicant has thus stated that locking is equivalent to the use of a PIN, and then argued why

the use of a PIN is unlike the instant method claims. Since the premise is untenable, the conclusion is irrelevant. "Encrypt" does not mean and is not equivalent to "the use of a PIN number to access information stored within the 'smart card', which cannot be accessed without the PIN number." Finally, the Examiner did not rely on the use of a PIN number in Davies for the rejection of the pertinent claim recitations. The Examiner in Paper #9 clearly relied upon the digital signature 16.

The Applicant extends this line of argument to the function of signing digital documents. These arguments are not persuasive because their premise remains faulty. Applicant states flatly in at page 7, in the second full paragraph that "There is not teaching or suggestion in Davies or Griffin that the element used to access used to access the information stored therein should then be transmitted to a remote location." Of course, this is not a repetition of the claim language. Instead, Davies teaches that the endorsed data is indeed transmitted to a remote location (i.e. a clearing house). On page 378, Davies teaches "A paper document of symbolic value can be called 'negotiable' in that it can be sold or given from one person to another, carrying its rights with it." Thus, when Davies writes a paper titled "Use of the 'Signature Token' to Create a Negotiable Document", it is highly unpersuasive to suggest that there is no teaching or suggestion that it can "be transmitted to a remote location". Clearly, when one person gives another person a negotiable document, and that person carries the negotiable document with them, then an endorsed transaction is transmitted to a remote location, e.g. wherever the second person is, or wherever the second person takes the document. Once the Applicant claims that "transmitted" is limited to transmission over networked computers, Examiner relies on Spies as an obvious extention of the Davies teachings. Until then, "transmitted" has many plain meanings which go beyond networked computers, and essentially encompasses all forms of transmission. Moreover, once the information is transmitted from one person to another over wires of any length, then that is the equivalent of transmission to a remote location, since the wires can be any length, and Applicant has not specified a minimum length to qualify as "remote".

Applicant then presents a dictionary definition to argue against the prior art references. Examiner points out that the dictionary definition supplied is not nearly as relevant as the claims interpreted in light of the specification. Examiner did not reject a dictionary definition of

"endorsement" but instead a "computer implemented method of generating secure endorsed transactions" recited in the preamble, as it would be understood by the skilled artisan. Davies expressly teaches "16 Signature of 9-15 by Customer" (see figure 1), where 9-15 is the transaction data. This signature creates a negotiable document which can be transmitted from person to person, and therefore from location to location.

Applicant also states that "The manifestations of the individual identifier of Griffin and the PIN number of Davies are used in order to initiate a process within the apparatus used. In contrast, the identifier of the present invention is used at a later time in order to confirm authenticity of the transaction in the form of an endorsement." Examiner respectfully disagrees. There is no real contrast. As explained above, the digital signature of Davies is negotiable, and is in fact used at a later time to confirm the authenticity of the transaction in the form of an endorsement. This is the whole point of Davies. A fair reading of the reference really should not fail to miss this aspect. Davies teaches the digital signature of a transaction to create a negotiable document. That document can be presented to a third party later, and its authenticity can be confirmed at that time using public key cryptography, without any need to contact the person or device which created the document. Again, this is the whole point of Davies. Griffith, moreover, contains consonant teachings in the specification. See for example, column 4, lines 62-67 of Griffith. "This method is employed to add to the transaction information set 404, 408, 409, and 410 a unique and verifiable authentication signature 411 and to verify such signatures when said information set 404, 408, 409, and 410 and signature reach the destination entity."

The Applicant makes other very similar arguments beginning at the end of page 8, through the first paragraph of page 9. These arguments are not persuasive for essentially the same considerations supplied above. In Davies, Even, and Griffith, there is in fact a later comparison of the negotiable document with a generated codes. This is the nature of the verification of the digital or authentication signature. Griffith would not refer to a "verifiable" authentication signature 411 were this not the case. Davies would not have defined "negotiable" as described above were this not the case.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Internet

PTO maintains an extensive web site at http://www.uspto.gov. Communications about this application via e-mail, other than those under 35 U.S.C. 132 or which otherwise require a signature, may be addressed to **mark.tremblay@uspto.gov**. All Internet e-mail communications will be recorded in the application. PTO employees don't use the Internet to exchange sensitive information unless the record includes a properly signed express waiver of the confidentiality requirements of 35 U.S.C. 122. For more details, see the Interim Internet Usage Policy published in the Official Gazette of the Patent and Trademark on February 25, 1997 at 1195 OG 89.

Voice

General inquiries or status inquiries about this application should be directed to the Group 2800 Receptionist at (703) 308-0956. Inquiries for the Examiner should be directed to Mark Tremblay at (703) 305-5176. The Examiner's regular office hours are 8:30 am to 6:00 pm EST Monday to Friday. Voice mail is available. If Applicant has trouble contacting the Examiner, the Supervisory Patent Examiner, Don Hajec, can be reached on (703) 308-4075. Technical questions and comments concerning PTO procedures may be directed to the Patent Assistance Center hotline at 1-800-786-9199 or (703) 308-4357.

Fax Procedures

Application papers may faxed to Art Unit 2876 at (703) 308-7724. Faxes must conform with the notice published in the Official Gazette, 1096 OG 30 (November 15, 1989). Papers solely for the examiner's consideration, and not intended for immediate entry into the application (e.g., a proposed amendment) should be unsigned and clearly marked "Draft Copy" and/or "Deliver Directly to Examiner."

MT

July 18, 1999

Donald Hajec
Supervisory Patent Examiner
Technology Center 2800